APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/477,107	12/31/1999	CHRISTOPHER L. HAMLIN	K35A0576	8721

			EXAMINER
26332	7590	10/30/2003	DADA, BEEMNET W

WESTERN DIGITAL CORP.
20511 LAKE FOREST DRIVE
C205 - INTELLECTUAL PROPERTY DEPARTMENT
LAKE FOREST, CA 92630

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No. 09/477,107	Applicant(s) HAMLIN, CHRISTOPHER L.
	Examiner Beemnet W Dada	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3-_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 1999* .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2,3 &4* .

4)☐ Interview Summary (PTO-413) Paper No(s). _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: .

DETAILED ACTION

All claims have been examined. Claims 1-14 are pending.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claim 1,3,8 and 10 are rejected under 35 U.S.C 102(e) as being anticipated by U.S. Patent No. 5,892,826 to Brown et al. (hereinafter referred to as Brown).

3. As per claim 1, Brown teaches, an integrated circuit for selectively encrypting data received from a device to send to another device. The integrated circuit comprising: a flexible encryption decryption circuitry having a first terminal (data input) a second terminal (data output) and a control input (enable input) (see column 6, lines 4-26). Brown shows the first terminal coupled with an internal data bus for receiving unencrypted data, the second terminal coupled with an external data bus for providing encrypted data. Furthermore, at column 3, lines 15-36, Brown shows an encryption determination circuit having an input terminal for receiving signal for validating a device;

an output terminal for providing a bypass signal (verification signal) to the encryption circuitry allowing the encryption circuitry to provide encryption.

4.   As per claim 8, Brown teaches, a method of controlling encryption circuitry for selectively encrypting data, the method having the steps of: receiving unencrypted data from a device, receiving signal for validating the device, (column 6, lines 4-23) and providing a bypass signal (verification signal) in response to receiving device validation signal, and allowing the encryption circuitry to provide encryption in response to the bypass signal. (column 6, lines 20-26)

5.   Claim 3 is rejected applied as above in rejecting claim 1. Furthermore Brown teaches, at column 3, lines 15-35, the encryption determination circuit, where the authentication signal comprises of an internal address (device identifier); and the encryption determination circuit verifies the device by comparing its internal address to corresponding predefined ranges of address.

6.   Claim 10 is rejected applied as above in rejecting claim 8. Furthermore Brown teaches, at column 3, lines 15-35, a method of selective encryption, where the authentication signal comprises of an internal address (device identifier), and the method of providing a bypass signal in response to the device validation signal comprises the steps of comparing the device's internal address to corresponding predefined ranges of address.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 4, 5, 6, 7, 11, 12, 13 and 14 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Brown in view of Lewis (U.S. Patent No. 5,734,819).

9.   Claim 4 is rejected applied as above in rejecting claim 3. Furthermore Brown

teaches an integrated circuit with flexible data encryption but does not explicitly teach

the concept of hardwiring device identifier into an integrated circuit. Lewis teaches, at

column 1, lines 45-60, a method where chip identifier can be programmed in a chip and

made non-changeable (hardwired), thereby teaching protection against duplication of

device serial numbers. Therefore it would have been obvious to one having ordinary

skill in the art at the time the invention was made to combine the teachings of Lewis

related to hardwired security and have modified the integrated circuit of Brown, because

such modification would provide protection against duplication of device serial numbers

by using multiple ways of hardwired security mechanism.

10.   Claim 5 is rejected applied as above in rejecting claim 3. Furthermore, Brown

teaches an integrated circuit with flexible data encryption but does not explicitly teach

storing device identifier in the second device, which is a non-volatile memory. Lewis

teaches, at column 1, lines 27-35, the method of storing device identifier in a non-

volatile memory, thereby teaching flexibility of use of non-volatile memory. Therefore it

would have been obvious to one having ordinary skill in the art at the time the invention

was made to modify the integrated circuit of Brown so as to include a non-volatile

memory to store data as per teachings of Lewis. One would have been motivated to

make such modification in view of the suggestion in Lewis that non-volatile memory

device gives flexibility to storing different serial numbers. Lewis shows that use of non-

volatile memory by a manufacturer would give the manufacturer flexibility to write

different serial number on each machine.

11.   Claim 6 is rejected applied as above in rejecting claim 1. Furthermore, Brown

teaches an integrated circuit with flexible data encryption but does not explicitly teach

the concept of generating message authentication code over plaintext data. Lewis

teaches, at column 2, lines 7-49, the method of generating message authentication

code over text data received from a device using a secret key and verifying the device

by verifying the message authentication code using a secret key, thereby teaching the

capability of detecting any duplication or modification of device identifier. Therefore it

would have been obvious to one having ordinary skill in the art at the time the invention

was made to modify the integrated circuit of Brown so as to include a message

authentication code generated over the plaintext data using the device key and further

verifying the message authentication code using an internal key as per teachings of

Lewis. One would have been motivated to make such modification in view of the

suggestion in Lewis that Message Authentication code can be used to detect duplication

or modification of serial number.

12.   Claim 7 is rejected applied as above in rejecting claim 1. Furthermore, Brown

teaches an integrated circuit with flexible data encryption having a device for processing

signals (see column 3, lines 1-15). Brown does not explicitly disclose the use of non-

volatile memory as the second device. Lewis teaches, at column 1, lines 27-35, the use

of non-volatile memory, thereby teaching the flexibility of use of non-volatile memory.

Therefore it would have been obvious to one having ordinary skill in the art at the time

the invention was made to further modify the integrated circuit of Brown so as to include

a non-volatile memory as per teachings of Lewis. One would have been motivated to

make such modification in view of the suggestion in Lewis that non-volatile memory

device gives flexibility to storing data. Lewis shows that use of non-volatile memory by a

manufacturer would give the manufacturer flexibility to write different serial number on

each machine.

13.   Claim 11 is rejected applied as above in rejecting claim 10. Furthermore, Brown

teaches an integrated circuit with flexible data encryption but does not explicitly teach

the concept of hardwiring device identifier into an integrated circuit. Lewis teaches, at

column 1, lines 45-60, a method where chip identifier can be programmed in a chip and

made non-changeable (hardwired), thereby teaching protection of duplication of device

serial numbers. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Lewis related to hardwired security and have modified the integrated circuit of Brown, because such modification would provide protection against duplication of device serial numbers. Lewis teaches multiple ways in which a unique chip identifier could be protected against duplication by hardwired security mechanism.

14.   Claim 12 is rejected applied as above in rejecting claim 10. Furthermore, Brown teaches an integrated circuit with flexible data encryption but does not explicitly teach storing the device identifier in the second device, which is a non-volatile memory. Lewis teaches, at column 1, lines 27-35, the concept of storing device identifier in a non-volatile memory, thereby teaching the flexibility of use of non-volatile memory. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify the integrated circuit of Brown so as to include a non-volatile memory to store data as per teachings of Lewis, So that the device identifier can be stored on the non-volatile memory. One would have been motivated to make such modification in view of the suggestion in Lewis that non-volatile memory device gives flexibility to storing different serial numbers. Lewis teaches that use of non-volatile memory by a manufacturer would give the manufacturer flexibility to write different serial number on each machine.

15.   Claim 13 is rejected applied as above in rejecting claim 8. Furthermore, Brown

teaches an integrated circuit with flexible data encryption but does not explicitly teach

the concept of generating message authentication code over plaintext data. Lewis

teaches, at column 2, lines 7-49, a method of generating message authentication code

over text data from a device using a secret key and verifying the device by verifying the

message authentication code using a secret key, thereby teaching the capability of

detecting any duplication or modification of device identifier. Therefore it would have

been obvious to one having ordinary skill in the art at the time the invention was made

to modify the integrated circuit of Brown so as to include a message authentication code

generated over the plaintext data using the device key and further verifying the

message authentication code using an internal key as per teachings of Lewis. One

would have been motivated to make such modification in view of the suggestion in

Lewis that Message Authentication code can be used to detect duplication or

modification of a serial number.

16.   Claim 14 is rejected applied as above in rejecting claim 8. Furthermore, Brown

teaches, at column 3, lines 1-15, an integrated circuit with flexible data encryption a

having a device for processing signals. Brown does not disclose the use of non-volatile

memory as the second device. Lewis teaches, at column 1, lines 27-35, the concept of

non-volatile memory, thereby teaching the flexibility of the use of non-volatile memory.

Therefore it would have been obvious to one having ordinary skill in the art at the time

the invention was made to modify the integrated circuit of Brown so as to include a non-

volatile memory as per teachings of Lewis. One would have been motivated to make

such modification in view of the suggestion in Lewis that non-volatile memory device

gives flexibility to storing data. Lewis shows that use of non-volatile memory by a

manufacturer would give the manufacturer flexibility to write different serial number on

each machine.

17.   Claims 2 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Brown in view of Le Rue (U.S. Patent No. 5,694,469).

18.   Claim 2 is rejected applied as above in rejecting claim 1. Furthermore, Brown

shows, at column 3, lines 15-36, an encryption determination circuit having an input

terminal for receiving signal for validating a device; an output terminal for providing a

bypass signal (verification signal) to the encryption circuitry allowing the encryption

circuitry to provide encryption. Brown does not teach two encryption determination

circuits used together to verify both the source and the destination devices. Le Rue

teaches, at column 4, lines 37-48, a method of verifying the source device and

destination device before allowing process to continue, thereby teaching an

enhancement of the authentication process. Therefore it would have been obvious to

one having ordinary skill in the art at the time the invention was made to combine the

teachings of Le Rue related to authentication the source and destination devices and

have modified the integrated circuit of Brown. One would have been motivated to make

such a modification in view of the suggestion in Le Rue that the security of the system

would be further enhanced by the fact that access is made based on authentication of both the source and destination devices.

19.   Claim 9 is rejected applied as above in rejecting claim 8. Furthermore, Brown teaches, at column 3, lines 15-36, a method of selective encryption, the method comprising; receiving signal for validating the device; providing a bypass signal (verification signal) in response to receiving device validation signal; and allowing the encryption circuitry to provide encryption. Brown does not teach two encryption determination circuits used together to verify both the source and the destination devices. Le Rue teaches, at column 4, lines 37-48, a method of verifying the source device and destination devices before allowing process to continue, thereby teaching an enhancement of the authentication process. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Le Rue related to authentication the source and destination devices and have modified the integrated circuit of Brown. One would have been motivated to make such a modification in view of the suggestion in Le Rue that the security of the system would be further enhanced by the fact that access is made based on authentication of both the source and destination devices.

Conclusion

20.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

a)   U.S. Patent No. 5,251,304 to Sibigtroth et al., discloses integrated circuit

microcontroller with on-chip memory and external bus interface and programmable

mechanism for securing the contents of on-chip memory.

b)   U.S. Patent No. 5,343,525 to Hung et al., discloses hard disk data security

device.

c)   U.S. Patent No. 6,073,236 to Kusakabe et al., discloses authentication method,

communication method, and information processing apparatus.

d)   U.S. Patent No. 6,036,0321 B1 to Gressel et al., discloses secure computer

system.

e)   U.S. Patent No. 6,304,658 B1 to kocher et al., discloses leak resistant

cryptographic method and apparatus.

f)   U.S. Patent No. 6,026,293 to Osborn, discloses a system for preventing

electronic memory tampering.

        Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Beemnet W Dada whose telephone number is (703)

305-8895. The examiner can normally be reached on Monday-Friday 8:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5486.

Beemnet Dada

October 23, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100